

STATEMENT OF STUART K. PRATT
ASSOCIATED CREDIT BUREAUS, INC.
WASHINGTON, D.C.

HEARING ON
PREVENTING IDENTITY THEFT BY TERRORISTS

Before the Subcommittee on Oversight and Investigations of the House Financial
Services Committee and the Subcommittee on Social Security of the House Ways and
Means Committee
of the
United States House of Representatives

Washington, D.C.

Thursday, November 8, 2001

Chairmen Kelly and Shaw, thank you for this opportunity to appear before this joint hearing of the House Financial Services Subcommittee on Oversight and Investigations and the House Ways and Means Subcommittee on Social Security. For the record, my name is Stuart Pratt and I am vice president government relations for Associated Credit Bureaus.

ACB as we are commonly known is an international trade association representing 500 consumer information companies that provide fraud prevention and risk management products, credit and mortgage reports, tenant and employment screening services, check fraud and verification services, and collection services.

We applaud your willingness to hold this important hearing on the subject of the Social Security Administration's Death Master File (DMF) and its uses for fraud prevention. It is clear, now more than ever, that nothing is more vital than ensuring that this country's public and private sector have every information tool necessary to prevent fraud and illegal access to services. The key to ensuring that both the government and the private sector can fully authenticate identifying information on applications of all types is through a robust system of authentication and verification technologies. At the core of these technologies is the availability of validated consumer identification information for cross-matching purposes. The social security number plays a particularly important role in the accuracy and completeness of this cross-matching process by allowing systems to be linked to ensure that all relevant records are considered when authenticating consumer data.

Congress has already recognized and begun to act on this need for strong and effective consumer information authentication measures through the enactment of the USA PATRIOT Act, which requires the Secretary of the Treasury to establish minimum standards for financial institutions, which must verify account applicant data.¹ Further evidence of the need to authenticate the identities of applicants was heard last week in your very timely hearing, Chairman Shaw, wherein we learned from the Inspector General of the Social Security Administration that they are reevaluating the authentication systems they will need to ensure that misuse of our social security account numbering system does not happen easily.

The subject of today's hearing, which focuses on the Social Security Administration's Death Master File, is a key component in this broad assessment of how we verify identities and prevent illegal access to products, entitlements and services. Let me now address some of the specific questions you raised in your letter of invitation.

How do consumer reporting agencies use the Social Security Administration's Death Master File?

In answering this question, the Committees should consider the scope of our members' coverage of the current U.S. market place. The three major credit reporting systems, Equifax, Experian and TransUnion, which provide nationwide coverage for all credit active Americans (approximately 200 million files per data base), are subscribers to the

¹ PL 107-56, Title III, Subtitle A, Section 326.

DMF. Nationwide coverage is also provided by other key ACB member company DMF subscribers including eFunds and Dolan Media. In sum total more than a billion consumer reports of various types, which can carry DMF notifications, are sold each year to depository institutions, creditors, telecommunications companies, the insurance industry and even to governmental agencies.

In terms of uses of the death master file, these include notifying users of various types of consumer reporting and identity verification/authentication products that a particular social security number is likely associated with a deceased individual. Our members' services include providing DMF notification in products sold (such as credit reports) and also sweeping customer data bases to ID records associated with DMF records. As you can see, our members' product offerings are extensive and far-reaching.

Are there technical problems identified with the current system of providing DMF data to ACB member subscribers?

ACB will look into this question with our DMF subscriber members and respond in more detail for the hearing record. One of our members, Dolan Media, indicated to us that the Social Security Administration has made significant improvement in the DMF over the past two years. Specifically they report that data in the DMF, which used to be outdated by as much as six month is now reported more often within 30 to 60 days of the death.

What other means of obtaining information about deceased individuals are available in order for ACB members to put a “hold” on SSNs?

As with the previous question, ACB will need time to fully develop our answer. It is our understanding that ACB credit reporting system members, which are also subscribers to the DMF, do receive, at least in some cases, notification of death from lenders and other regular furnishers of information to our members’ data bases. These notifications are included in special comment fields and codes, which are standardized through the association’s data reporting format standard, Metro2. These comment codes are available to subsequent users of consumer credit reports.

Can you outline ways in which sources of information can be better integrated to prevent fraudulent uses of social security numbers?

Our members’ systems are a good example of how the private sector is already integrating a range of information sources today. Key in this integration is the freedom to develop fraud prevention products for a range of industries.

Unfortunately, for example, the current FTC rules issued as a result of the enactment of the Gramm-Leach-Bliley Act (GLB) seriously impinge on the use of essential consumer identifying information for non-Fair Credit Reporting Act purposes. Due to the FTC interpretation of GLB, credit header data² is restricted even for use by other financial

² The term “credit header information” commonly includes information such as name, address, previous address, telephone number, and social security number.

institutions. But beyond GLB or permitted uses for consumer reports under the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), under the FTC GLB rules, credit header is not available for eCommerce authentication products, location and verification of pension fund recipients, and a host of other uses which are not covered under either law. In fact, the rule may foreclose on any opportunity to use credit header for other types of security screening efforts, such as scanning airline passenger manifests.

Said differently, we need to ensure that current laws and regulations, including GLB, do not interfere with efforts to more fully integrate information sources for fraud prevention and general identity verification, in particular, where the use of credit header would take place outside of the Fair Credit Reporting Act or the Gramm-Leach-Bliley Act.

Can you identifying steps the consumer reporting agencies are taking to update their systems to prevent fraudulent uses of the SSN.

We need more time to answer this question completely. However, we are very pleased to announce in support of your hearing that all of our members identified to date as subscribers to the DMF are ensuring that their systems are programmed to accept monthly updates of the DMF from the Social Security Administration. In fact, a majority of our members are already subscribers to the Social Security Administration's DMF monthly updates. This operational change by our members should ensure that our members' data is as updated as possible and in turn will allow creditors and other

subscribers to our members' systems to more effectively authenticate applicant information, including the social security number and prevent fraud.

Further, in closing my remarks, I am pleased to announce that ACB will create a new Task Force consisting of all members of the association which are also subscribers to the Social Security Administration's DMF. This task force will serve as a liaison with the Social Security Administration on technology and legal issues as they continue their own assessment of how best to deliver DMF data to subscribers.

Thank you again for this opportunity to appear before your committees. We support your efforts and I am happy to answer any questions.